ORACLE®

Oracle Access Management 12c

Assurance Activity Report

Version 1.0

July 2023

Document prepared by

Lightship Security

www.lightshipsec.com

Table of Contents

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security for the evaluation identified in Table 1. The AAR is produced in accordance with National Information Assurance Program (NIAP) reporting guidelines.

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Scheme	Canadian Common Criteria Scheme
Evaluation Facility	Lightship Security
Developer/Sponsor	Oracle Corporation
TOE	Oracle Access Management 12c, build 12.2.1.4 with patches 35371374 and 33974688
Security Target	Oracle Access Management 12c Security Target, v1.9
Protection Profile	Standard Protection Profile for Enterprise Security Management Policy Management (PP_ESM_PM), v2.1 Standard Protection Profile for Enterprise Security Management Access Control (PP_ESM_AC), v2.1

1.2 Evaluation Methods

2 The evaluation was performed using the methods and standards identified in Table 2.

Table 2: Evaluation Methods

<table>
<tr><td><b>Evaluation Criteria</b></td><td>CC v3.1R5</td></tr>
<tr><td><b>Evaluation Methodology</b></td><td>CEM v3.1R5</td></tr>
<tr><td><b>Interpretations</b></td><td>
<table>
<tr><th colspan="2">ESM PM and applicability</th></tr>
<tr><td>TD0042 Removal of Low-level Crypto Failure Audit from PPs</td><td>Applicable</td></tr>
<tr><td>TD0055 Move FTA_TAB.1 to Selection-Based Requirement</td><td>Applicable</td></tr>
<tr><td>TD0066 Clarification of FAU_STG_EXT.1 Requirement in ESM PPs</td><td>Applicable</td></tr>
<tr><td>TD0079 RBG Cryptographic Transitions per NIST SP 800-131A Revision 1</td><td>Applicable</td></tr>
</table>
</td></tr>
</table>

TD0573 Update to FCS_COP and FCS_CKM in ESM PPs	Applicable
TD0574 Update to FCS_SSH in ESM PPs	Not applicable. The TOE does not implement SSH.
TD0576 FTP_ITC and FTP_TRP Updated	Applicable
TD0621 Corrections to FCS_TLS_EXT.1 in ESM PPs	Applicable

ESM AC and applicability	
TD0042 Removal of Low-level Crypto Failure Audit from PPs	Applicable
TD0066 Clarification of FAU_STG_EXT.1 Requirement in ESM PPs	Applicable
TD0079 RBG Cryptographic Transitions per NIST SP 800-131A Revision 1	Applicable
TD0573 Update to FCS_COP and FCS_CKM in ESM PPs	Applicable
TD0574 Update to FCS_SSH in ESM PPs	Not applicable. The TOE does not implement SSH.
TD0576 FTP_ITC and FTP_TRP Updated	Applicable
TD0621 Corrections to FCS_TLS_EXT.1 in ESM PPs	Applicable

1.3 Reference Documents

Table 3: List of Reference Documents

Ref	Document
[ST]	Oracle Access Management 12c Security Target, v1.9
[AGD]	Oracle Access Management 12c Common Criteria Guide, Version 1.5
[AGD-Online]	Administering Oracle Access Management (online guide) https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/introduction-oracle-access-management.html

Ref	Document
[PM]	Standard Protection Profile for Enterprise Security Management Policy Management, October 24, 2013, Version 2.1
[AC]	Standard Protection Profile for Enterprise Security Management Access Control, October 24, 2013, Version 2.1

2 Assurance Activities for ESM Policy Management

2.1 Class ESM: Enterprise Security Management

2.1.1 ESM_ACD.1 Access Control Policy Definition

2.1.1.1 TSS

3 The evaluator shall do the following:

- Verify that the TSS identifies one or more compatible Access Control products

- Verify that the TSS describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)

- Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the Standard Protection Profile for Enterprise Security Management Policy Management ““policies the Access Control products are capable of consuming

- Verify that the TSS indicates how policies are identified

Findings:

- [ST] Section 6.1.1 defines the WebGate as a compatible access control product.

- [ST] Section 6.1.1 defines the scope and granularity of policies: “The TOE is an integrated product that provides both Policy Management and Access Control capabilities, so there are no compatibility considerations for the ability to define policies. Every single operation that the Access Control component is capable of controlling is something that can be defined in a policy by the Policy Management component. Therefore, the subjects, objects, and operations against which a WebGate is capable of controlling access to is the same set of subjects, objects, and operations that can be defined in a policy by the OAM Console.”

- The evaluator verified that this [ST] is for the Access Control product as well as the Policy Manager, and that there is a correspondence between the policies created and the consumption of the policies.

- [ST] Section 6.1.1: WebGate policies are identified by a unique name and each policy artifact is identified by a unique UID.

2.1.1.2 Guidance Documentation

4 The evaluator shall review the operational guidance to ensure that that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE.

Findings:

[AGD] Section 1.3.4 specifies in Table 2 that the ESM Access control product is the OAM Server and OAM WebGate. [AGD] Section 3.5 specifies the allowable content and specifies that a policy ID is associated with each Authorization Policy.

This is consistent with the [ST].

2.1.1.3 Tests

5 The evaluator shall test this capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.

High-Level Test Description
Using the OAM Console define policies for consumption on the OAM Server and OAM WebGate.
The following subjects will be used: *organizational users defined in Identity Store.* The Identity Store is specified in Configuration > User Identity store.
The following objects will be used: *URLs, files, executable scripts.* These objects will be specified within a specific Application Domain.
The following operations will be used: *Allow or Deny Access.* These operations will be specified on the Resource definition page and associated with a specific object.
The following attributes will be used: *attributes associated with organizational users defined in Identity Store.* These will be associated with a policy on the authorization policy conditions page associated with a specific resource.
The policy will be transmitted to the policy store for consumption by the OAM Server and subsequent transmission of the policy decisions to the OAM WebGate.
The policy store will be reviewed for the policy identifier.
Using a browser test to ensure that the policy has been transmitted to the OAM WebGate by attempting to access the specified resource.
The policy will need to be modified to show use of each of the objects and possible attributes.
Findings: PASS

2.1.2 ESM_ACT.1 Access Control Policy Transmission

2.1.2.1 TSS

6 The evaluator shall check the TSS and ensure that it summarizes when and how policy data will be transmitted to Access Control products. This includes the ability to specify the product(s) that the policy data will be sent to.

Findings:	[ST] Section 6.3.1: When an administrator on the OAM Console creates or modifies an access control policy, the policy data is immediately transmitted to the environmental Policy Store for future retrieval by the OAM server. The updated policy data is then queried by the WebGate when a user attempts to access a protected resource.

2.1.2.2 Guidance Documentation

7 The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable).

Findings:	The [AGD] specifies in section 3.5 the means to create and update policies.

The [AGD] section 1.3.3 specifies that the “WebGates will poll the OAM Server for relevant policy data when a user attempts to access a protected resource” as well as “WebGates will periodically poll the server for new policy information”.

Additionally, the [AGD-Online] provides extensive information on the management of policies in Section 25 “Managing Policies to Protect Resources and Enable SSO”.

2.1.2.3 Tests

8 The evaluator shall test this capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then, following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator shall create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words,

a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed;

b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic interval has passed, and then confirm that the new policy is present in the Access Control component; or

c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified “other circumstances”, then a similar test shall be executed to confirm transmission under those circumstances.

9 The evaluator shall then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.

10 The evaluator shall repeat this test for a representative sample of Access Control products that can be managed by the TOE. For example, if the TOE provides the ability to manage groups of host-based access control endpoints, the evaluator shall create different groups such that each supported platform is included in at least one group and verify that group members will appropriately consume policies when instructed to do so.

11 Note: This testing will likely be performed in conjunction with the testing of ESM_ACD.1.

High-Level Test Description
As noted in the test case for ESM_ACD.1 the transmitted policy will be modified and verified that the modified policy is enforced by the OAM Server and OAM WebGate. Update the policies by deleting the policy from the TOE and verify that the default policy is enforced.
Findings: PASS

2.1.3 ESM_EAU.2 Reliance on Enterprise Authentication

2.1.3.1 TSS

12 The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.

Findings:	[ST] Section 6.5.2: The OAM Console component defines individual users who exist in the environmental Identity Store as administrators for the TOE. Administrators will supply authentication credentials (username/password) to the TOE which then relays the authentication request to the Identity Store.

2.1.3.2 Guidance Documentation

13 The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication.

Findings:	The evaluator notes that the [AGD-Online] 4.2 About Delegating the Identity Store specifies that the TOE uses an LDAP directory defined as the System Identity Store to authenticate administrators to the OAM console.

2.1.3.3 Tests

14 The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.

15 Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).

High-Level Test Description
Attempt to login to the TOE using invalid, or no authentication information and verify the TOE denies access.
Findings: PASS

2.1.4 ESM_EID.2 Reliance on Enterprise Identification

16 This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

2.2 Class FAU: Security Audit

2.2.1 FAU_GEN.1 Audit data generation

2.2.1.1 TSS

17 The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.

Findings:	[ST] Section 6.4.1 : Audit data is generated by the TOE for both administrative activity and for access attempts made against environmental resources that are mediated by the TOE. The startup and shutdown of the TOE is logged as part of the function of the application servers on which the TOE components reside. Actions performed by administrators on the OAM Console are logged to the Audit Store. Since WebGates query policy data from the Policy Store when user requests are performed, OAM auditing is all performed by the server component.

2.2.1.2 Guidance Documentation

18 The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record.

19 Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

20 The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

Findings:	The [AGD-Online] section 8 “Auditing Administrative and Run-time Events” provides a list auditable events. The [AGD-Online] section 8 “Auditing Administrative and Run-time Events” and section 9 “Logging WebGate Event Messages” provide the audit record format, and a description of each field. The evaluator found that the information was consistent with that required in FAU_GEN.1.2 and table 3 of the [AC] and the [PM]. The [AGD] Section 3.7 Log Types and Formats also provides sample audit entries for the start and completion of the logging services. The [AGD] Section 3.5 specifies that the TOE associates the policy ID is associated with a policy in the logs. The [AGD] and [AGD-Online] specify the two main ways in which to configure the TOE interfaces: the use of configuration files on the TOE platform and the use of the web-based user interface. .

2.2.1.3 Tests

21 The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

22 This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

High-Level Test Description
This testing has been conducted throughout the evaluation. The TOE has been shown to generate all required audit records with the required content.
Findings: PASS

2.2.2 FAU_SEL_EXT.1 External Selective Audit

2.2.2.1 TSS

23 The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing.

Findings:	[ST] Section 6.4.2: The events that are audited by OAM access control functionality are dependent on its configuration. The TSF has a configurable audit level with four settings: NONE, LOW, MEDIUM, and ALL.

2.2.2.2 Guidance Documentation

24 The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.

Findings:	The [AGD-Online] section 8.2.2 "About Oracle Access Management Auditing Configuration" specifies the use of audit filters to change the audit events captured. "Audit policies (known as Filter Presets declare the types of events to be captured by the audit framework for particular components." This is consistent with the [ST].

2.2.2.3 Tests

25 The evaluator shall test this capability by configuring a compatible Access Control product to have:

- All selectable auditable events enabled

- All selectable auditable events disabled
- Some selectable auditable events enabled

26 For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product.

27 If this SFR is iterated, the evaluator shall repeat these activities for each iteration of the SFR, substituting the appropriate external entity for “Access Control product” where appropriate.

High-Level Test Description
Login to the OAM Console and navigate to Configuration > Common Settings and modify the Filter Preset settings and verify that the setting changes the audit records which are written to the audit store.
Findings: PASS

2.2.3 FAU_STG_EXT.1 External Audit Trail Storage

2.2.3.1 TSS

28 The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.

Findings:	[ST] Section 6.4.5 : Audit records that are generated by the TSF are transmitted to the underlying local file systems in the Operational Environment and are not stored within the TSF. This data is also transmitted to the Audit Store in the evaluated configuration but the OAM Console does not provide the ability to modify or delete audit data stored in this manner. [ST] Section 6.4.5 specifies the use of TLS for the audit store connection.

2.2.3.2 Guidance Documentation

29 The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

Findings:	The [AGD] specifies that the audit logs transmitted to the underlying local file systems and a database in the Operational Environment and are not stored within the TSF. Section 3.4 of the [AGD] specifies the location of the audit logs. Section 3.4.2 specifies the configuration of the audit database, and provides information on how data is passed and what happens upon a connection loss and re-establishment.

2.2.3.3 Tests

30 The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one

High-Level Test Description
Verify audit data is flowing to the audit store database by generating audit data and reviewing the contents on the database virtual machine. The use the virtual machine settings to disconnect the ethernet connection between the TOE and the audit store. Generate audit data on the TOE by logging in and logging out. Enable the ethernet connection on the database server virtual machine. Review the audit data and verify that the previously generated log in and log out audit events are present in the audit store.
Findings: PASS

2.3 Class FIA: Identification and Authentication

2.3.1 FIA_USB.1 User-Subject Binding

2.3.1.1 TSS

31 The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.

Findings:	[ST] Section 6.5.7: Once an administrator is authenticated to the TOE, they are provided with a session cookie that associates their web browser with the authenticated session. This session is uniquely identified so that the authenticated administrator is associated with only the data that applies to their own session. The administrator is defined in terms of username, role, and administrative scope so that only authorized actions can be performed against the TSF.

2.3.1.2 Guidance Documentation

32 The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.

Findings:	The [AGD-Online] Section 4.2 About Delegating the Identity Store specifies that the System Identity Store is used to enforce authentication during the execution of the administrative operations. The [AGD-Online] Section 5.4.2 Defining and Removing Administrator Roles specifies the steps to map the TOE roles to use System Identity Store defined users or groups.

2.3.1.3 Tests

33 The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.

High-Level Test Description
Login as a system administrator and configure the TOE to associate two different domain admin groups with specific application domains. Login to the TOE as a user in each of the groups and verify access to different application domains, as well as limited access compared to the system administrator.
Findings: PASS

2.4 Class FMT: Security Management

2.4.1 FMT_MOF.1 Management of Functions Behavior

2.4.1.1 TSS

34 The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.

Findings:	The evaluator verified that the assignments in FMT_SMF and FMT_SMR align with the assignments in FMT_MOF. Additionally, the [ST] Section 6.1.3 specifies "Within the administrative interface, the super administrator has the ability to define domains and assign WebGates to these domains. They can then define domain administrators that are only able to administer policies within those domains."

2.4.1.2 Guidance Documentation

35 The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.

Findings:	The [AGD-Online] section 4.1 "Understanding Administrator Roles" specifies a role-based restriction of management authority between the System Administrator and the Application Domain Administrator. The [AGD-Online] specifies that the System Administrator has access to the entire TOE configuration and the Application Domain Administrator is limited to policy creation and resources associated with a specific application domain.

	The [AGD-Online] section 4.3 "Assigning Roles Using the Administration Console" specifies the delegation of administration roles is done by assigning an user, or group.

2.4.1.3 Tests

36 The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

High-Level Test Description
Login to the TOE as a super administrator and domain administrator and verify the differing levels of access. Verify that the level of access is consistent with the [ST], and [AGD-Online]. The TOE cannot be configured by an authorized and compatible Secure Configuration Management product.
Findings: PASS

2.4.2 FMT_MOF_EXT.1 External Management of Functions Behavior

2.4.2.1 TSS

37 The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions.

Findings:	The evaluator verified that the assignments in FMT_SMF and FMT_SMR align with the assignments in FMT_MOF_EXT. Additionally, the [ST] Section 6.1.3 specifies "The TSF provides the ability for administrators to configure WebGates as well as the ability to configure the OAM Console. All administration is performed using the OAM Console."

2.4.2.2 Guidance Documentation

38 The evaluator shall check the operational guidance in order to determine that it provides instructions for how to connect to an Access Control product and what privileges are required to perform management functions on it once the connection has been established.

Findings:	The [AGD-Online] section 15.2 "OAM Agent Registration Parameters in the Console" provides instructions on how to connect WebGate(s). The [AGD-Online] section 15.5 "Configuring and Managing Registered OAM Agents Using the Console" provides instructions on the management of a WebGate.

2.4.2.3 Tests

39 The evaluator shall test this capability by deploying the TOE in an environment where there is an Access Control component that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

40 The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:

- Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function’s behavior and observe that the audit repository now logs (or doesn’t log) this event based on the modified behavior

- Repository for audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository

- Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.

- Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.

- Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.

41 Once this has been done, the evaluator shall reconfigure the TOE so that it is no longer authorized to manage the Access Control product. The evaluator shall then attempt to perform management functions using the TOE and observe that this is either disallowed or that the option is not even present

High-Level Test Description
Using the OAM console verify that the configuration of the TOE also impacts the OAM server and WebGate. This includes modification of the audit level and audit storage, verification of differing levels of access, configuration of access control through domain administrator settings, configuration of policies, and settings for the OAM WebGates and OAM Server.
Findings: PASS

2.4.3 FMT_MSA_EXT.5 Consistent Security Attributes

2.4.3.1 TSS

42 The evaluator shall review the TSS and in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur. If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion.

Findings:	[ST] Section 6.1.4 specifies the rules which are applied to resolve or prevent conflicting policies for instance “When an administrator defines an authorization policy, the presence of explicitly contradictory rules (e.g. the same subject-object-operation combination at the same level of detail results in both a permit and a deny result) will prevent the policy from being saved”.

2.4.3.2 Guidance Documentation

43 If the TOE requires manual intervention in order to resolve contradictory policy data, the evaluator shall review the operational guidance in order to verify that it provides a summary of contradictory policy situations and the steps that must be taken in order to resolve them. If the TOE’s policy engine prevents such contradictions, the evaluator shall review the operational guidance in order to verify that it describes how the TSF reconciles any contradictory policy data (such as different rules simultaneously allowing and denying a certain behavior).

Findings:	The [AGD] specifies in section 3.5.1 that if an administrator defines explicitly contradictory rules (e.g. the same subject-object-operation combination at the same level of detail results in both a permit and a deny result) will prevent the policy from being saved.

2.4.3.3 Tests

44 The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature shall be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.

High-Level Test Description
Using the OAM console edit an authorization policy to include contradictory conditions. Verify that the TOE will prevent the authorization policy from being saved. Using the OAM console edit an application domain to define resources with the same level of specificity to include contradictory conditions. Verify that the TOE will deny access to the resource. Using the OAM console define precedence levels and verify the first applicable policy is applied. Change the levels of precedence and verify that the TOE applies the new first applicable policy.
Findings: PASS

2.4.4 FMT_SMF.1 Specification of Management Functions

45 The security management functions for FMT_SMF.1 are distributed throughout the cPP and are included as part of the requirements in FTA_SSL_EXT.1, FTA_SSL.3, FTA_TAB.1, FMT_MOF.1/ManualUpdate, FMT_MOF.1/AutoUpdate (if included in the ST), FIA_AFL.1, FIA_X509_EXT.2.2 (if included in the ST), FPT_TUD_EXT.1.2 & FPT_TUD_EXT.2.2 (if included in the ST and if they include an administrator-configurable action), FMT_MOF.1/Services, and FMT_MOF.1/Functions (for all of these SFRs that are included in the ST), FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.

2.4.4.1 TSS

46 The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.

Findings: [ST] Section 6.5.1 specifies the management functions available.

2.4.4.2 Guidance Documentation

47 The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.

Findings: The [AGD-Online] provides guidance on all of the management functions as noted below:

Creation of policies: Section 25.2.3 Creating or Managing an Application Domain and Policies provides links to all the relevant guidance sections describing the creating and management of policies on the TOE.

Transmission of policies: Policies are transmitted to the OAM server immediately after policy creation. There is no configuration options for the transmission of policies.

Definition of object attributes: Section 25.5.1 Resources in an Application Domain specifies the definition of the resource protection level and provides a link to Section 25.5.1.4 Query String Name and Value Parameters for Resource Definitions which allows for administrator-defined-attributes.

Association of attributes with objects: Object attributes are implicit as the attributes are defined on a page associated with the object. Attributes are not independently defined.

N/A – Authentication data is managed by the environmental Identity Store and not the TSF (ESM_EAU.2)

N/A – Authentication data is managed by the environmental Identity Store and not the TSF (ESM_EID.2)

Configuration of auditable events: Section 8.5.3 Using the Oracle Access Management Console for Audit Configuration, specifies the use of the OAM console to configure audit settings in a manner consistent with the [AGD].

Configuration of auditable events for defined external entities: Section 9 Logging WebGate Event Messages includes the subsections which includes the configuration of log levels in Section 9.2.2 Log Configuration File Contents.

Configuration of external audit storage location: The TOE does not store any audit data. Audit data is transmitted to a database and the local file system. The configuration of the transmission of the audit data to the database is specified in Section 8.5.1 Setting Up the Audit Database Store.

Definition of subject security attributes, modification of subject security attributes: Section 5.4.2 Defining and Removing Administrator Roles specifies the steps to map the TOE roles to use System Identity Store defined users or groups.

Configuration of the behavior of other ESM products: Section 15 Registering and Managing OAM Agents covers the ability to manage other ESM products. The OAM agent considered for this evaluation is limited to the OAM WebGate.

Management of sets of subjects that can interact with security attributes: Section 5.4.2 Defining and Removing Administrator Roles specifies the steps to map the TOE roles to use System Identity Store defined users or groups. In this context it is limiting the administrators who are able to define policies for the WebGates.

Management of rules by which security attributes inherit specified values: Section 25 Managing Policies to Protect Resources and Enable SSO and associated subsections provides guidance on the configuration of policies and security rules mapped to WebGates.

N/A – the TSF automatically behaves in the secure manner defined by this SFR and this behavior is not configurable (FMT_MSA.5)

Management of the users that belong to a particular role: Section 5.4.2 Defining and Removing Administrator Roles specifies the steps to map the TOE roles to use System Identity Store defined users or groups. In this context it is associating users with the Domain Admin role or the System Administrator role.

N/A – this SFR was moved to selection-based as per NIAP TD0055 and has not been included within the scope of the TOE (FMT_TAB.1)

N/A – the actions requiring the use of a trusted channel are not configurable once the TOE is in an operational state: The developer configures the trusted channel on behalf of the customer as indicated in the [AGD]. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services. (FTP_ITC.1)

N/A – the actions requiring the use of a trusted path are not configurable once the TOE is in an operational state: The developer configures the trusted path on behalf of the customer as indicated in the [AGD]. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services. (FTP_TRP.1)

2.4.4.3 Tests

48 The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability.

High-Level Test Description
Login to the OAM Console and use the interface and exercise the management functions. Verify that the TOE allows for the management functions to be performed.
Findings: PASS

2.4.5 FMT_SMR.1 Security Management Roles

2.4.5.1 TSS

49 The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.

Findings: [ST] Section 6.5.3 The OAM Console has a super administrator role that has full control over the TSF. Additionally, the ability to interact with policies can be granted to domain administrators by associating those administrators with specific domains.

This is consistent with the SFR.

2.4.5.2 Guidance Documentation

50 The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.

Findings: The [AGD-Online] specifies the ability to define administrator roles based on LDAP Username or LDAP group. The [AGD-Online] further specifies the use of the Weblogic LDAP server as the primary LDAP server for the definition of administrative users and roles.

“By default, the Oracle Access Management Administrators role is the same as the WebLogic Administrators role (Administrators).

“You can register another User Identity Store (Oracle Internet Directory, for example); however, user WebLogic must be defined with at least one user in the registered store to authenticate against. Administrator login works only when the Authentication Scheme (and assigned Authentication Module), also uses the System Store.”

https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/managing-data-sources.html#GUID-54797F4B-6367-40CE-80D4-8079EBF9DDFD

2.4.5.3 Tests

51 The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.

High-Level Test Description
Login as a system administrator and configure the TOE to associate two different domain admin groups with specific application domains. Login to the TOE as a user in each of the groups and verify access to different application domains, as well as limited access compared to the system administrator.
Findings: PASS

2.5 Class FPT: Protection of the TSF

2.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

2.5.1.1 TSS

52 The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.

Findings:	[ST] Section 6.5.4 The TOE uses identity and credential data that is defined in the operational environment Identity Store in order to authenticate administrators and to identify end users. This data is not persistently stored by the TOE or retained by the TSF after an authentication attempt has been made, so there is no dedicated interface to the TOE that can be used to disclose administrator credential data.

2.5.1.2 Guidance Documentation

53 There are no operational guidance activities for this SFR.

Findings:	NA

2.5.1.3 Tests

54 The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.

High-Level Test Description
Login to the TOE’s underlying operating system as a root user and use grep to search for password data in the configuration files. Login to the OAM console and present queries to the credential repositories to attempt to cause passwords to be displayed. Login to the credential repository as root and attempt to output passwords.
Findings: PASS

2.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

2.5.2.1 TSS

55 The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the

application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Findings: [ST] Section 6.5.5 The TOE provides no interface to view secret key data. The cryptographic data used by the TOE is protected against unauthorized disclosure by the cryptographic modules in the environment that are used by the TOE to secure remote communications.

2.5.2.2 Guidance Documentation

56 There are no operational guidance or testing activities for this SFR.

Findings: NA

2.5.2.3 Tests

57 There are no operational guidance or testing activities for this SFR.

Findings: NA

2.6 Class FTP: Trusted path/channels

2.6.1 FTP_ITC.1 Inter-TSF trusted channel

2.6.1.1 TSS

58 [Modified by TD0576] The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Findings: [ST] Section 6.3.4 specifies TLS is used to secure communications with authorized IT entities. The evaluator also verified that URLs are used to assure the identification of the non-TSF endpoint. The evaluator verified that the TLS related SFRs are included in the [ST].

2.6.1.2 Guidance Documentation

59 [Modified by TD0576] The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Findings: The [AGD] specifies that the TOE will be configured with the support of the developer. This includes the configuration of the trusted channels. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services.

2.6.1.3 Tests

60 [Modified by TD0576] The evaluator shall perform the following tests:

61 Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Note	The TOE is configured with the assistance of the developer. The connections are configured to use TLS. Additionally, the ciphersuites are limited in the evaluated configuration.

62 Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the Oracle-DB machine and restart the service to clear out TLS session information (which will force a new handshake). Attempt to access a protected resource using a predefined LDAP user and a bad password. Examine Wireshark and verify that the TOE initiates TLS communications with the Oracle-DB and LDAP and inter-TOE endpoints. Examine Wireshark and verify that the traffic is encrypted.
Findings: PASS

63 Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Note	The TOE maintains trusted channels over TLS and to the local OS. These channel is constantly tested throughout the evaluation. Using Wireshark the evaluator verified that the channel data is not sent in plaintext as verified in Test 2.

64 Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

65 Further assurance activities are associated with the specific protocols.

66 For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

High-Level Test Description
Engage Wireshark over the interface being tested. Physically disconnect the interface (disconnect from the remote end rather that from the TOE end to ensure that the TOE is unable to invoke any layer 2 carrier-sensing mechanism). Wait 5 seconds. Physically reconnect the cable. Examine Wireshark and verify that the log interface continues to send encrypted Application Data packets.

High-Level Test Description
Findings: PASS

2.6.2 FTP_TRP.1 Trusted Path

2.6.2.1 TSS

67 [Modified by TD0576] The evaluator shall check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path and ensure they are consistent with those declared in the ST. In addition, the evaluator shall ensure that the TSS adequately describes the way the trusted communication path is protected.

68 The evaluator shall also check the TSS to ensure that the ST author specifies whether remote administration is applicable to the TOE and if applicable, specifies all the methods of remote administration, along with how those communications are protected.

Findings:	[ST] Section 6.5.6 specifies TLS is used. The evaluator verified that the TLS related SFRs are included in the [ST].

2.6.2.2 Guidance Documentation

69 [Modified by TD0576] The evaluator shall confirm that the guidance documentation contains instructions for how users will interact with the TOE such as a web application via HTTPS. The evaluator shall also ensure that the guidance documentation discusses the mechanism by which a trusted path to the TOE is established and which environmental components (if any) the TSF relies on to assist in this establishment.

Findings:	The [AGD] specifies that the TOE will be configured with the support of the developer. This includes the configuration of the trusted paths. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services.

2.6.2.3 Tests

70 [Modified by TD0576] The evaluator shall perform the following tests:

71 Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Note	The TOE is configured with the assistance of the developer. The connections are configured to use TLS. Additionally, the ciphersuites are limited in the evaluated configuration.

72 Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

High-Level Test Description
Engage Wireshark over the appropriate interface.

High-Level Test Description
Log into the trusted path. Examine Wireshark and verify that the trusted path sends encrypted traffic after any initial plaintext protocol negotiation occurs.
Findings: PASS

73 Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Note	The TOE maintains two trusted channels over TLS. This channel is constantly tested throughout the evaluation. Using Wireshark the evaluator verified that the channel data is not sent in plaintext as verified in the previous test case.

74 Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

75 Further assurance activities are associated with the specific protocols.

76 For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

High-Level Test Description
Engage Wireshark over the interface being tested. Physically disconnect the interface (disconnect from the remote end rather that from the TOE end to ensure that the TOE is unable to invoke any layer 2 carrier-sensing mechanism). Wait 5 seconds. Physically reconnect the connection to the web server. Examine Wireshark and verify that the log interface continues to send encrypted Application Data packets.
Findings: PASS

77

3 Architectural Variations and Additional Requirements Policy Management

3.1 Attribute Definition

3.1.1 ESM_ATD.1 Object Attribute Definition

3.1.1.1 TSS

78 The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.

Findings: [ST] Section 6.1.2 For web servers that are protected by WebGates, “An administrator can associate URL and file objects with a required authentication level. The URL is configured in two parts: the host identifier which provides the domain name, and the resource identifier which provides the path to a specific resource.”

3.1.1.2 Guidance Documentation

79 The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.

Findings: The [AGD-Online] specifies the creation and management of Host Identities associated with the URLs in Section 22.4 Managing Host Identifiers.

The [AGD-Online] specifies the creation and management of Resources associated with the URLs in Section 25.5 Adding and Managing Policy Resource Definitions.

3.1.1.3 Tests

80 The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.

High-Level Test Description
Using the OAM Console define an Authorization policy custom attribute for a protected resource protected by an OAM WebGate and verify that access is permitted or denied based on the attribute.
Findings: PASS

3.2 Selectable Auditing

3.2.1 FAU_SEL.1 Selective Audit

3.2.1.1 TSS

81 The evaluator shall check the TSS in order to determine that it discusses the TSF’s ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing.

Findings:	[ST] Section 6.4.2: The events that are audited by OAM access control functionality are dependent on its configuration. The TSF has a configurable audit level with four settings: NONE, LOW, MEDIUM, and ALL.

3.2.1.2 Guidance Documentation

82 The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.

Findings:	The [AGD-Online] specifies the available logging level settings in Section 7.2.3 About Logging Levels. The [AGD-Online] further specifies the configuration of the logging levels in Section 7.3 Configuring Logging for Access Manager.

3.2.1.3 Tests

83 The evaluator shall test this capability by using all allowable vectors that are defined in FMT_MOF.1 to configure the TOE in the following manners:

- All selectable auditable events enabled
- All selectable auditable events disabled
- Some selectable auditable events enabled

84 For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.

High-Level Test Description
Login to the OAM Console and navigate to Configuration > Common Settings and modify the Filter Preset settings and verify that the setting changes the audit records which are written to the audit store.
Findings: PASS

3.3 Cryptographic Functional Requirements

3.3.1 FCS_HTTPS_EXT.1 HTTPS

3.3.1.1 TSS

85 The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality.

Findings:	[ST] Section 6.7.1: The TOE provides the ability for remote administrators to connect to the OAM Console using HTTPS as specified in RFC 2818. This HTTPS implementation uses TLS as described in [AC+PM] FCS_TLS_EXT.1. When an

	administrator accesses the TOE using a web browser, the HTTPS connection is established through the web server (using RSA BSAFE) that is used by the TSF to serve web content remotely. Only after the HTTPS connection is established can the administrator supply authentication credentials to the TOE.

3.3.1.2 Guidance Documentation

86 There are no assurance activities to be performed against the operational guidance for this requirement.

Findings:	NA

3.3.1.3 Tests

87 Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

High-Level Test Description
The TLS testing has passed therefore this testing requirement has passed.
Findings: PASS

3.3.2 FCS_TLS_EXT.1 TLS

3.3.2.1 TSS

88 [Modified by TD0575 and TD0621] The evaluator shall check the TSS to ensure that it describes whether the TOE acts as a TLS server, TLS client, or both and map this to specific trusted path/channel cases. If a specific TLS application is not part of the evaluated configuration, the TSS shall identify it, specifically declare it as out of scope, and declare whether it is disabled by default.

89 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component.

Findings:	[ST] Section 6.7.2 includes table 21 which lists the TLS channels used and when the TOE is acting as the client or server. Section 6.7.2 also includes a list of claimed ciphersuites which match those claimed for the component.

3.3.2.2 Guidance Documentation

90 [Modified by TD0575] The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the product so that TLS conforms to the description in the TSS. If administrative steps need to be taken to disable a specific TLS application or so that the cipher suites negotiated by the implementation are limited to those in this requirement, then the appropriate instructions need to be contained in the guidance.

Findings:	The [AGD] specifies that the TOE will be configured with the support of the developer. This includes the configuration of the trusted channels and trusted paths. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services.

3.3.2.3 Tests

91 [Modified by TD0575] The evaluator shall also perform the following tests for each use of TLS in the TOE (as defined in the TSS):

92 Test 1: The evaluator shall establish a TLS connection using each claimed cipher suite specified by the requirement. It is sufficient to observe the successful handshake following the negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to negotiate all specifically claimed ciphersuites.
Findings: PASS

93 Test 2: The evaluator shall perform the following modifications to the Client/Server Hellos:

94 Test 2a: [conditional on TOE implementing TLS client] The evaluator shall send a Server Hello containing only the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the TOE denies the connection.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server using the TLS_NULL_WITH_NULL_NULL (cipher ID 0x0000).
Findings: PASS

95 Test 2b: [conditional on TOE implementing TLS Server] The evaluator shall send a Client Hello containing only the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the TOE denies the connection.

High-Level Test Description
Using a Lightship developed TLS client, force the TOE server to attempt a handshake with a test client using TLS_NULL_WITH_NULL_NULL (cipher ID 0x0000).
Findings: PASS

96 Test 3: The evaluator shall perform the following modifications to the traffic:

97 Test 3a: [conditional on TOE implementing TLS client]

98 Test 3a.1: Change the TLS version sent in the Server Hello to an undefined TLS version (for example 1.5 represented by the two bytes 03 06) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS server, connect to the TOE and attempt to negotiate an invalid TLS protocol version.

High-Level Test Description
Findings: PASS

99 Test 3a.2: Change the TLS version sent in the Server Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS server, connect to the TOE and attempt to negotiate SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 any unsupported, but otherwise valid TLS protocol versions contained in the PP.
Findings: PASS

100 Test 3a.3: If DHE or ECDHE cipher suites are supported, modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the handshake is not completed and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a modified nonce value. Do this once for a DHE and ECDHE key exchange ciphersuite.
Findings: PASS

101 Test 3a.4: [conditional] If DHE or ECDHE cipher suites are supported, modify the signature block in the server's Key Exchange handshake message, and verify that the handshake does not complete and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled key exchange signature.
Findings: PASS

102 Test 3a.5:

103 Test 3a.5a: Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client does not complete the handshake and no application data flows.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a non-negotiated ciphersuite.
Findings: PASS

104 Test 3a.5b: Modify a byte in the Server Finished handshake message and verify the client does not complete the handshake and no application data flows.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled finished message.
Findings: PASS

105 Test 3a.5c: Send a garbled message from the server after the server has issued the Change Cipher Spec message and verify that the client does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 …).

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled message after the ChangeCipherSpec and verify no application data is sent.
Findings: PASS

106 **Test 3b**: [conditional on TOE implementing TLS server]

107 **Test 3b.1**: Change the TLS version sent in the Client Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE and attempt to negotiate TLS 1.1 protocol and verify the TOE rejects the connection.
Findings: PASS

108 Test 3b.2:

109 **Test 3b.2a**: Modify a byte in the data of the client's Finished handshake message and verify the server rejects the connection and does not send any application data.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE and modify the first payload byte in the Client Finished message.
Findings: PASS

110 **Test 3b.2b**: Demonstrate that the TOE will not resume a session for which the client failed to complete the handshake (independent of TOE support for session resumption). Generate a Fatal Alert by sending a Finished message from the client before the client sends a ChangeCipherSpec message, and then send a ClientHello with the session identifier from the previous incomplete session and verify the server does not resume the session.

High-Level Test Description
Perform a successful handshake using one of the accepted ciphersuites and verify that the Server Finished message is encrypted.
Findings: PASS

111 **Test 3b.2c**: Send a garbled message from the client after the client has issued the Change Cipher Spec message and verify that the server does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 …).

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE server to attempt a handshake with a test client sending a mangled message after the ChangeCipherSpec and verify no application data is sent.
Findings: PASS

4 Assurance Activities for ESM Access Control

4.1 Class ESM: Enterprise Security Management

4.1.1 ESM_EID.2 Reliance on Enterprise Identification

4.1.1.1 TSS

112 The evaluator shall check the TSS and ensure that it describes where the subject identity data that the TOE uses to make access control decisions comes from. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each identification mechanism that is used by the TSF.

Findings:	[ST] Section 6.2.3 Both administrators who manage the TOE and end users who access objects that are protected by the TSF are identified by username data that is defined in the environmental Identity Store prior to any TSF-mediated actions being allowed.

4.1.1.2 Guidance Documentation

113 There are no Operational Guidance activities for this SFR.

Findings:	NA

4.1.1.3 Tests

114 This SFR is not separately tested; appropriate behavior of the access control SFP is sufficient to assert that accurate subject identity data is received by the TOE.

High-Level Test Description
Attempt to access a resource protected by the TOE and verify that the TOE uses the LDAP server to authenticate the access.
Findings: PASS

4.2 Class FAU: Security Audit

4.2.1 FAU_GEN.1 Audit Data Generation

4.2.1.1 TSS

115 The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.

Findings:	[ST] Section 6.4.1 : Audit data is generated by the TOE for both administrative activity and for access attempts made against environmental resources that are mediated by the TOE. The startup and shutdown of the TOE is logged as part of the function of the application servers on which the TOE components reside.

Actions performed by administrators on the OAM Server are logged to the Audit Store. Since WebGates query policy data from the Policy Store when user requests are performed, OAM auditing is all performed by the server component.

4.2.1.2 Guidance Documentation

116 The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

117 The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

Findings: The [AGD-Online] specifies the each of the audit events in Section 8.3 Access Manager Events You Can Audit. The evaluator verified that each audit event mandated by the PP is described and has the required information.

The [AGD-Online] specifies all the available settings for the audit configuration in Section 7.3 Configuring Logging for Access Manager.

4.2.1.3 Tests

118 The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

119 This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

High-Level Test Description
This testing has been conducted throughout the evaluation. The TOE has been shown to generate all required audit records with the required content.
Findings: PASS

4.2.2 FAU_SEL.1 Selective Audit

4.2.2.1 TSS

120 The evaluator shall check the TSS in order to determine that it discusses the TSF’s ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing.

Findings:	[ST] Section 6.4.2: The events that are audited by OAM access control functionality are dependent on its configuration. The TSF has a configurable audit level with four settings: NONE, LOW, MEDIUM, and ALL.

4.2.2.2 Guidance Documentation

121 The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.

Findings:	The [AGD-Online] Section 8.4 Identity Federation Events You Can Audit specifies the ability to configure the audit level. The selections here are consistent with the selections specified in the ST.

4.2.2.3 Tests

122 The evaluator shall test this capability by using a compatible ESM Policy Management or ESM Secure Configuration Management product to configure the TOE in the following manners:

- All selectable auditable events enabled
- All selectable auditable events disabled
- Some selectable auditable events enabled

123 For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.

High-Level Test Description
Login to the OAM Console and navigate to Configuration > Common Settings and modify the Filter Preset settings and verify that the setting changes the audit records which are written to the audit store.
Findings: PASS

4.2.3 FAU_STG.1 Protected Audit Trail Storage (Local Storage)

4.2.3.1 TSS

124 The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally, what happens when the local audit data store is full, and how these records are protected against unauthorized access.

Findings:	[ST] Section 6.4.4 : Audit records that are generated by the TSF are transmitted to the underlying local file systems in the Operational Environment and are not stored within the TSF.

4.2.3.2 Guidance Documentation

125 The evaluator shall examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and ―cleared‖ periodically by sending the data to the audit server.

Findings:	The [AGD] Section 3.4 Audit Logging specifies that no audit data is stored by the TOE but is sent to the underlying OS and to the Audit Store as configured. The [AGD-Online] Section 8.2.3 About Audit Record Storage clarifies that the TOE supports the use of local bus stop files as well as the transfer of audit data to a database.

4.2.3.3 Tests

126 The evaluator shall test this capability by attempting to access locally-stored audit data without authorization and observe that the attempts fail. They shall also observe that the space allocated for audit storage is consistent with the TSF's capabilities.

High-Level Test Description
The TOE does not provide an interface to the underlying OS files. Using a browser attempt to access the files on the underlying OS using path traversal techniques.
Findings: PASS

4.2.4 FAU_STG_EXT.1 External Audit Trail Storage

4.2.4.1 TSS

127 The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.

Findings:	[ST] Section 6.4.4 : Audit records that are generated by the TSF are transmitted to the underlying local file systems in the Operational Environment and are not stored within the TSF. This data is also transmitted to the Audit Store in the evaluated configuration but the OAM Console does not provide the ability to modify or delete audit data stored in this manner. [ST] Section 6.4.5 specifies the use of TLS for the audit store connection.

4.2.4.2 Guidance Documentation

128 The evaluator shall check the operational guidance in order to determine that it lists any configuration steps required to set up audit storage. If audit data is stored in a remote repository, the evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

Findings:	The [AGD] Section 4.1 FIPS & TLS Setup and Configuration specifies that the setup of the TLS channel should be done with developer assistance and the configuration is specified in [AGD-Online] Appendix B.

4.2.4.3 Tests

129 The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.

High-Level Test Description
Verify audit data is flowing to the audit store database by generating audit data and reviewing the contents on the database virtual machine. Then use the virtual machine settings to disconnect the ethernet connection between the TOE and the audit store. Generate audit data on the TOE by logging in and logging out. Enable the ethernet connection on the database server virtual machine. Review the audit data and verify that the previously generated log in and log out audit events are present in the audit store.
Findings: PASS

4.3 Class FCO: Communication

4.3.1 FCO_NRR.2 Enforced proof of receipt

4.3.1.1 TSS

130 The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it discusses how the TOE identifies itself to the Policy Management product and how it provides evidence of the policy's consumption to the Policy Management product.

Findings:	The evaluator verified that the SFR assignments are completed in a manner that is consistent with the applications notes. [ST] Section 6.3.2: As part of setting up a WebGate, a unique ID and credentials are defined for it. WebGate policies are identifiable by a unique name and every policy is further given a unique UID so that different versions of the same policy can be differentiated from one another. [ST] Section 6.3.2: Each WebGate identifies the name and ID of the policy that is being implemented.

4.3.1.2 Guidance Documentation

131 The evaluator shall check the operational guidance in order to determine how the TOE confirms evidence of received policy data back to the Policy Management product that originally sent it that policy data. This should include the contents and formatting of the receipt such that the data that it contains is verifiable.

Findings:	The [AGD] specifies in section 3.5 that "The policy ID is associated with the policy at policy creation and modification in the TOE logs. The policy is written to the policy store and the OAM server retrieves the policy from the policy store. The OAM Server

pushes a list of all active policy IDs to the shared policy database, each time a change in policies is made. The policy data is written to the policy store in an Oracle proprietary format."

This list of active policies allows for confirmation of receipt of policy data.

4.3.1.3 Tests

132 The evaluator shall test this capability by configuring an environment such that the TOE is allowed to accept a policy from a certain source, sending it a policy from that source, observing that the policy is subsequently consumed, and that an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST. The evaluator confirms accuracy by using the Policy Management product to view the receipt and ensure that its contents are consistent with known data.

High-Level Test Description
The evaluator reviewed the database and verified that the OAM server specifies a policy read and lists all active policies on the OAM server.
Findings: PASS

4.4 Class FDP: User Data Protection

4.4.1 FDP_ACC.1 Access Control Policy

133 Specific assurance activities are defined for each technology type in Appendix C.1.

134 If the TSF enforces multiple distinct types of access control policies, the evaluator shall also ensure that the SFRs for each policy are properly iterated in the ST and that all of the assurance activities for each individual iteration are satisfied.

135 Note: The PP includes the FDP_ACC.1 SFR in the mandatory requirements as a placeholder for the SFR which is specified in section 5.1.1 in this Assurance Activity Report. As such it is replicated here.

4.4.2 FDP_ACF.1 Access Control Functions

136 Refer to FDP_ACC.1 above.

137 Note: The PP includes the FDP_ACF.1 SFR in the mandatory requirements as a placeholder for the SFR which is specified in section 5.1.2 in this Assurance Activity Report. As such it is replicated here.

4.5 Class FMT: Security Management

4.5.1 FMT_MOF.1(1) Management of Functions Behavior

4.5.1.1 TSS

138 The evaluator shall check the TSS in order to determine that it summarizes how the management functions described in the SFR are performed (or, if their behavior is fixed, why this is the case) and how the TSF determines that the management request is authorized.

Findings:	The evaluator verified that the assignments in FMT_SMF and FMT_SMR align with the assignments in FMT_MOF.

4.5.1.2 Guidance Documentation

139 The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with a Policy Management product and how that product is subsequently used to manage the TOE.

Findings:	The [AGD-Online] Section 15 Registering and Managing OAM Agents specifies the process for the registration and subsequent management of WebGates.

4.5.1.3 Tests

140 The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

141 The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:

- Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function’s behavior and observe that the audit repository now logs (or doesn’t log) this event based on the modified behavior

- Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository

- Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.

- Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.

- Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.

142 Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy

Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.

High-Level Test Description
Using the OAM console verify that the configuration of the TOE also impacts the OAM server and WebGate. This includes modification of the audit level and audit storage, verification of differing levels of access, configuration of access control through domain administrator settings, configuration of policies, and settings for the OAM WebGates and OAM Server.
Findings: PASS

4.5.2 FMT_MOF.1(2) Management of Functions Behavior

4.5.2.1 TSS

143 The evaluator shall check the TSS in order to determine that it indicates the ESM products (or distributed TOE components if multiple ESM PPs are claimed) that are authorized to query the TOE and that this includes, at minimum, a Policy Management component.

Findings:	[ST] Section 6.2.5 The TOE uses assurance of endpoints in order to ensure that communications between the OAM Server and WebGates only occurs when they are authorized as part of the same deployment. Specifically, WebGates can define a credential during their registration.

4.5.2.2 Guidance Documentation

144 The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with other ESM products and why these other products are used to interface with the TSF.

Findings:	The [AGD-Online] Section 15 Registering and Managing OAM Agents specifies the process for the registration and subsequent management of WebGates. The [AGD] and [AGD-Online] clearly specify that the OAM Console is used to define access control policies which are then distributed to WebGates by the OAM Server.

4.5.2.3 Tests

145 The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to query the policy being implemented by the TOE.

146 Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.

High-Level Test Description
Verify that the TOE is protecting a resource, then disconnect TOE from the Policy Store.

High-Level Test Description
Login to the OAM Console and attempt to deploy policies and verify that the OAM Server is not possible to be managed.
Findings: PASS

4.5.3 FMT_MSA.1 Management of Security Attributes

4.5.3.1 TSS

147 The evaluator shall review the TSS and the operational guidance to confirm that the indicated attributes are maintained by the TOE.

Findings:	[ST] Section 6.2.5 lists the security attributes as follows: Access Control Policies Access Control Policy Attributes Implementation status of access control policies.

4.5.3.2 Guidance Documentation

148 The evaluator shall also confirm that the operational guidance defines how authorizations to manage the defined security attributes are derived so that an administrator will know how to configure separation of duties.

Findings:	The [AGD-Online] makes it clear in Section 23.2 Overview of the SSO Login Process with OAM Agents and ECC that the OAM Server maintains the Access Control Policies, Access Control Policy Attributes, and Implementation status of access control policies. The OAM server transmits this information to the WebGate when a user attempts to access a resource. The [AGD-Online] also clearly specifies the use of application domains, and association between the domain administrator and the application domain in Section 4 Delegating Administration. These two sections provide the ability to define security attributes and the separation of duties.

4.5.3.3 Tests

149 The evaluator shall test this capability by using the associated Policy Management product to confirm that each identified operation against the indicated attributes may be performed, and that the TOE interfaces do not provide the ability for any other roles to perform operations against the indicated attributes.

High-Level Test Description
This is tested as part of FMT_SMR.1 and FIA_USB.1. This product is a combined policy management and access control TOE. The management of the product and roles associated are the same.
Findings: PASS

4.5.4 FMT_MSA.3 Static Attribute Initialization

4.5.4.1 TSS

150 The evaluator shall review the TSS in order to determine how the TSF puts restrictive default values into place (for example, access control policies should operate in deny-by-default mode so that the absence of an access control rule doesn't fail to restrict an operation) and what authorizations are required in order to override these defaults.

Findings:	[ST] Section 6.2.6: By default, the TOE implements a restrictive access control policy against objects that are defined to be protected.

4.5.4.2 Guidance Documentation

151 The evaluator shall review the operational guidance in order to ensure that it warns the reader of the restrictive nature of default values and provides instructions on how to override them.

Findings:	[AGD] Section 3.5.2 Default Values specifies that "By default, the TOE implements a restrictive access control policy against objects that are defined to be protected. If no policy exists for an object, it is out of scope of the TOE as the TSF is not aware that the object exists. Administrators can opt to define access control rules for these objects that are more permissive in nature, either by explicitly allowing access to certain subjects based on certain conditions, or by excluding some operations from enforcement."

4.5.4.3 Tests

152 The evaluator shall test this capability by using the associated Policy Management product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value and that it can be overridden in the manner specified by the operational guidance.

High-Level Test Description
Using the OAM Console remove all define attributes from the Allowed rules for a specified protected resource. Verify that the TOE denies access if no allow rules are defined. Add conditions to the Allow rule section for the object and verify that a user is able to access the rule for each of the associated attributes.
Findings: PASS

4.5.5 FMT_SMF.1 Specification of Management Functions

4.5.5.1 TSS

153 The evaluator shall check the TSS in order to determine what Policy Management and Secure Configuration Management product(s) (if applicable) are compatible with the TOE.

Findings:	[ST] Section 6.5.1: The TOE includes the OAM Console as the management interface which controls the access control components. The evaluator verified that the TOE includes a Policy Management which is compatible.

4.5.5.2 Guidance Documentation

154 The evaluator shall check the operational guidance in order to ensure that it describes how to configure the TOE to interface with the compatible products discussed in the TSS. The evaluator shall also check the operational guidance to verify that it provides instructions for performing each of the defined management functions.

Findings:	Please refer to the assessment in Section 2.4.4.2 of this document.

4.5.5.3 Tests

155 The evaluator shall test this capability by configuring the TOE in a manner that is consistent with the evaluated configuration. For each management function that has been defined in the ST, the evaluator shall perform the function in a manner that is consistent with the operational guidance and verify that the observed behavior is consistent with the expectations of what the function should accomplish.

High-Level Test Description
Login to the OAM Console and use the interface and exercise the management functions. Verify that the TOE allows for the management functions to be performed.
Findings: PASS

4.5.6 FMT_SMR.1 Security Roles

4.5.6.1 TSS

156 The evaluator shall examine the TSS to verify that it describes how management authority is delegated via one or more roles and how an authorized Policy Management product is associated with those roles.

Findings:	[ST] Section 6.5.3 The OAM Console has a super administrator role that has full control over the TSF. Additionally, the ability to interact with WebGates can be granted to domain administrators by associating those components with specific domains. This is consistent with the SFR.

4.5.6.2 Guidance Documentation

157 The evaluator shall review the operational guidance in order to verify that it discusses the various administrative role(s) that are used to manage the TSF and any applicable steps that are required for an administrator to assume such a role.

Findings:	The [AGD-Online] Section 4.2 About Delegating the Identity Store specifies the use of System Identity Store to enforce authentication during the execution of the administrative operations. The [AGD-Online] Section 5.4.2 Defining and Removing Administrator Roles specifies the steps to map the TOE roles to use System Identity Store defined users or groups.

4.5.6.3 Tests

158 The evaluator shall use the associated Policy Management product to connect to the TOE and confirm that it is operating in the assigned role. The evaluation shall also

confirm that a user or other external entity that has not been authorized for the indicated role cannot assume the indicated role.

High-Level Test Description
Login as a system administrator and configure the TOE to associate two different domain admin groups with specific application domains. Login to the TOE as a user in each of the groups and verify access to different application domains, as well as limited access compared to the system administrator.
Findings: PASS

4.6 Class FPT: Protection of the TSF

4.6.1 FPT_APW_EXT.1 Protection of Stored Credentials

4.6.1.1 TSS

159 The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.

Findings:	[ST] Section 6.5.4 The TOE uses identity and credential data that is defined in the operational environment Identity Store in order to authenticate administrators and to identify end users. This data is not persistently stored by the TOE or retained by the TSF after an authentication attempt has been made, so there is no dedicated interface to the TOE that can be used to disclose administrator credential data.

4.6.1.2 Guidance Documentation

160 There are no operational guidance activities for this SFR.

Findings:	NA

4.6.1.3 Tests

161 The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.

High-Level Test Description
Login to the TOE’s underlying operating system as a root user and use grep to search for password data in the configuration files.

High-Level Test Description
Login to the OAM console and present queries to the credential repositories to attempt to cause passwords to be displayed. Login to the credential repository as root and attempt to output passwords.
Findings: PASS

4.6.2 FPT_FLS_EXT.1 Failure of Communications

4.6.2.1 TSS

162 The evaluator shall check the TSS in order to determine that it describes how the SFP(s) defined in FDP_ACC.1 are enforced when the TOE cannot communicate with the Policy Management product that provided the enforced policy. If communications are not expected to be severed (for example, if the TOE and Policy Management product run on the same system), the evaluator shall check the TSS in order to determine that this assertion has been made. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the failure state behavior is documented in sufficient detail to be unambiguously verifiable.

Findings:	[ST] Section 6.6.2: Any disruption in communication between the WebGate(s) and OAM Server, or between the OAM Server and Policy Store will result in access requests being denied during the outage.

4.6.2.2 Guidance Documentation

163 The evaluator shall check the operational guidance (and developmental evidence, if available) in order to determine that it discusses how the TOE is deployed in relation to other ESM products. This is done so that the evaluator can determine the expected behavior if the TOE is unable to interact with its accompanying Policy Management product.

Findings:	The [AGD] Section 3.6 Communication Failures specifies that if the OAM Server cannot access the policy store, or the OAM WebGate cannot access the OAM Server, the default action is to deny access.

4.6.2.3 Tests

164 The evaluator shall test this capability by terminating the Policy Management product (if the TOE resides on the same system) or by severing the network connection between the Policy Management product and the TOE (if the TOE resides on a different system). The evaluator shall then interact with the TOE while these communications are suspended in order to determine that the behavior it exhibits in this state is consistent with the expected behavior. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the observed behavior corresponds to its description in the TSS.

High-Level Test Description
The evaluator will disable access to the policy store and attempt to access a protected resource. Verify that the TOE denies access to the resource if the policy store is not accessible.
Findings: PASS

4.6.3 FPT_RPL.1 Replay Detection

4.6.3.1 TSS

165 The evaluator shall check the TSS in order to determine that it describes the method by which the TSF detects replayed data. For example, it may provide a certificate or other value that can be validated by the TSF to verify that the policy is consistent with some anticipated schema. Alternatively, the TOE may use a protocol such as SSL for transmitting data that immunizes it from replay threats.

Findings:	[ST] Section 6.8.3: The TOE uses TLS to immunize itself from replay threats.

4.6.3.2 Guidance Documentation

166 If the method of replay detection is configurable, the evaluator shall check the operational guidance in order to determine that it provides instructions for setting up and configuring the replay detection mechanism. This may be simple (e.g. setting up and enabling a TLS channel with shared secret) or complex (e.g. defining specific policy attributes that are positively associated with unauthorized changes), depending on how specifically replay detection is implemented by the TSF.

Findings:	The [AGD] Section 1.3.3 Evaluated Functions specifies that all communications associated with the transmission of policies are secured by TLS.

4.6.3.3 Tests

167 The evaluator shall test this capability by configuring replay detection in a manner specified by the operational guidance (if applicable), running a packet sniffer application (such as Wireshark) on the local network with the TOE, sending a valid policy to it, and observing the packets that comprise this policy. The evaluator can then take these packets and re-transmit them to the TOE. Once this has been done, the evaluator shall execute an appropriate subset of User Data Protection testing with the expectation that the policy enforced will be the first policy transmitted. If the expected results are met, the TOE is sufficiently resilient to rudimentary policy forgery.

High-Level Test Description
Using Wireshark verify that the TOE transmits all data via TLS.
Findings: PASS

4.6.4 FPT_SKP_EXT.1 Protection of Secret Key Parameters

4.6.4.1 TSS

168 The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Findings:	[ST] Section 6.5.5 The TOE provides no interface to view secret key data. The cryptographic data used by the TOE is protected against unauthorized disclosure by the cryptographic modules in the environment that are used by the TOE to secure remote communications.

4.6.4.2 Guidance Documentation

169 There are no operational guidance or testing activities for this SFR.

Findings: NA

4.6.4.3 Tests

170 There are no operational guidance or testing activities for this SFR.

Findings: NA

4.7 Class FRU: Resource Utilization

4.7.1 FRU_FLT.1 Degraded Fault Tolerance

4.7.1.1 TSS

171 The evaluator shall check the TSS in order to determine that describes how the TSF ensures that it is enforcing the most up-to-date policy. If an a malicious user was able to disconnect their system and the TOE misses a policy update from Policy Management during this outage, it is expected that the updated policy will be received once communications are resumed.

Findings: [ST] Section 6.6.1: If communications between the WebGate and the server components fail, the WebGate will periodically attempt to query the server in order to determine whether or not updated policy information is available. This allows the most recent policy to be enforced within a reasonable period of time once a communications outage is resolved.

4.7.1.2 Guidance Documentation

172 The evaluator shall check the operational guidance in order to verify that it discusses how the TSF receives the latest policy from the Policy Management product once a communications failure has been resolved, including any options that an administrator has in configuring this capability.

Findings: The [AGD] Section 3.6 Communication Failures specifies that the OAM Server (Policy Decision Point) will retrieve the latest policy from the Policy Store following the restoration of communications in the event of an outage.

4.7.1.3 Tests

173 The evaluator shall test this capability by severing the network connection between the TOE and the Policy Management product, defining an updated policy, and reestablishing the connection will determine if the TOE appropriately receives the new policy data within the time interval specified in FCO_NRR.2.3. The evaluator shall devise a scenario such that the old policy allows a specific action and that the new policy denies that same action. The evaluator shall then perform that action, observe that it is allowed, sever connection with the Policy Management product, define the new policy during that outage, re-establish the connection, wait for the interval defined by FCO_NRR.2.3, perform the same action again, and observe that it is no longer allowed.

High-Level Test Description
The evaluator will disable access to the policy store and attempt to access a protected resource. The TOE is expected to deny access to the resource if the policy store is not accessible. The evaluator will re-establish access to the policy store then disable the ethernet port on the OAM Server and attempt to access a protected resource. The TOE is expected to deny access to the resource.
Findings: PASS

4.8 Class FTP: Trusted Paths/Channels

4.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

4.8.1.1 TSS

174 [Modified by TD0576] The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Findings:	[ST] Section 6.3.4 specifies TLS is used to secure communications with authorized IT entities. The evaluator verified that the TLS related SFRs are included in the [ST].

4.8.1.2 Guidance Documentation

175 [Modified by TD0576] The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Findings:	The [AGD] specifies that the TOE will be configured with the support of the developer. This includes the configuration of the trusted channels and trusted paths. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services.

4.8.1.3 Tests

176 [Modified by TD0576] The evaluator shall perform the following tests:

177 Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Note	The TOE is configured with the assistance of the developer. The connections are configured to use TLS. Additionally the ciphersuites are limited in the evaluated configuration.

178 Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the Oracle-DB machine and restart the service to clear out TLS session information (which will force a new handshake). Attempt to access a protected resource using a predefined LDAP user and a bad password. Examine Wireshark and verify that the TOE initiates TLS communications with the Oracle-DB and LDAP and inter-TOE endpoints. Examine Wireshark and verify that the traffic is encrypted.
Findings: PASS

179 Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Note	The TOE maintains trusted channels over TLS and to the local OS. These channel is constantly tested throughout the evaluation. Using Wireshark the evaluator verified that the channel data is not sent in plaintext as verified in Test 2.

180 Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

181 Further assurance activities are associated with the specific protocols.

182 For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

High-Level Test Description
Engage wireshark over the interface being tested. Physically disconnect the interface (disconnect from the remote end rather that from the TOE end to ensure that the TOE is unable to invoke any layer 2 carrier-sensing mechanism). Wait 5 seconds. Physically reconnect the remote logging server. Examine wireshark and verify that the log interface continues to send encrypted Application Data packets.
Findings: PASS

5 Architectural Variations and Additional Requirements Access Control

5.1 Web-Based Access Control

5.1.1 FDP_ACC.1 Access Control Policy

5.1.1.1 TSS

183 None defined.

Findings:	NA

5.1.1.2 Guidance Documentation

184 None defined.

Findings:	NA

5.1.1.3 Tests

185 None defined.

Findings:	NA

5.1.2 FDP_ACF.1 Access Control Functions

5.1.2.1 TSS

186 The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy enforcement mechanism is described.

Findings:	[ST] Section 6.2.2: Each authorization policy includes the following: a) Unique name b) Success and failure URLs (where the subject's browser is redirected based on the access control decision) c) List of objects to which the authorization policy applies The evaluator verified that the TOE is capable of mediating the activities defined in Table 6.

5.1.2.2 Guidance Documentation

187 The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 16 above.

188 The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced.

Findings:	The [AGD-Online] Section 25.5 Adding and Managing Policy Resource Definitions specifies the ability to define resources (URLS) and operations (Allow or Deny Access) permitted to access those URLS. These resources have an associated authentication policy and authorization policy which is specified in sections 25.9 Introduction to Authorization Policy Rules and Conditions, and 25.10 Defining Authorization Policy Conditions. Subsection 25.10.2 Defining Identity Conditions specifies the ability to define rules based on a user. The [AGD] Section 3.5 specifies "The policy is written to the policy store and the OAM server retrieves the policy from the policy store." The AGD also specifies that the policy data is written in an Oracle proprietary format.

5.1.2.3 Tests

189 The evaluator shall then use an authorized and compatible Policy Management product to define policies that contain rules for mediating these activities. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities.

190 For example, consider the following combinations:

- authorized users/groups (subject), http://www.test.url (object), access via HTTP operation (operation), 1:00 PM (attribute)

191 The evaluator could test this combination by deploying a policy that allows a certain user and a certain group the ability to access http://www.test.url in their web browser between the hours of 9:00 AM and 5:00 PM. They can then log in as that user and observe that they are allowed to access the website at 1:00 PM. They can then test other aspects of this combination in the following manner:

- logging in as a different user and observing that they are not allowed to access the website
- assigning the unauthorized user to the group that is authorized to access the website and observing that they can now access it themselves
- accessing a different website that is not allowed by the policy and observing that this site cannot be accessed
- accessing the same website at 5:30 PM and observing that their access attempt is rejected due to the time attribute

192 This activity is then repeated for each other subject/object/operation/attribute combination.

High-Level Test Description
Using the OAM Console define policies for consumption on the OAM Server and OAM WebGate. The following subjects will be used: organizational users defined in Identity Store. The Identity Store is specified in Configuration > User Identity store. The following objects will be used: URLs, files, executable scripts. These objects will be specified within a specific Application Domain.

High-Level Test Description
The following operations will be used: Allow or Deny Access. These operations will be specified on the Resource definition page and associated with a specific object. The following attributes will be used: attributes associated with organizational users defined in Identity Store. These will be associated with a policy on the authorization policy conditions page associated with a specific resource. Verify that the policy is enforced by the OAM Server and OAM WebGate by attempting to access resources for which the TOE mediates access. Create authorization conditions for the policies to allow and deny access based on time, IP address and administrator defined conditions.
Findings: PASS

5.2 Conditional Enforcement of Session Establishment

5.2.1 FTA_TSE.1 TOE Session Establishment

5.2.1.1 TSS

193 The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined.

Findings:	[ST] Section 6.2.4: As part of its access control policy enforcement, a WebGate can enforce denial of session establishment by limiting a subject's access to a protected resource based on day or time.

5.2.1.2 Guidance Documentation

194 The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

Findings:	The [AGD-Online] Section 25.10.4 Defining Temporal Conditions specifies the ability to create Authorization Policies which limit the ability to authenticate to specific times of day.

5.2.1.3 Tests

195 The evaluator shall test this capability by performing positive and negative testing for each attribute that can be used to conditionally allow session establishment. For example, if a time of day restriction applies, the evaluator shall successfully log on during an acceptable time and shall be prevented from logging on during an unacceptable time.

High-Level Test Description
Configure an Authorization Policy condition and rule to deny connections based on the time of day. Verify that the rule is enforced by attempting to access a protected resource. The TOE will deny access. Modify the rule to apply to a different time of day, and verify access to the protected resource is available..
Findings: PASS

5.3 Cryptographic Functional Requirements

5.3.1 FCS_HTTPS_EXT.1 HTTPS

5.3.1.1 TSS

196 The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality.

Findings:	[ST] Section 6.7.1: The TOE provides the ability for remote administrators to connect to the OAM Console using HTTPS as specified in RFC 2818. This HTTPS implementation uses TLS as described in [AC+PM]FCS_TLS_EXT.1. When an administrator accesses the TOE using a web browser, the HTTPS connection is established through the web server (using RSA BSAFE) that is used by the TSF to serve web content remotely. Only after the HTTPS connection is established can the administrator supply authentication credentials to the TOE.

5.3.1.2 Guidance Documentation

197 There are no assurance activities to be performed against the operational guidance for this requirement.

Findings:	NA

5.3.1.3 Tests

198 Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

Findings:	NA

5.3.2 FCS_TLS_EXT.1 TLS

5.3.2.1 TSS

199 [Modified by TD0575] The evaluator shall check the TSS to ensure that it describes whether the TOE acts as a TLS server, TLS client, or both and map this to specific trusted path/channel cases. If a specific TLS application is not part of the evaluated configuration, the TSS shall identify it, specifically declare it as out of scope, and declare whether it is disabled by default.

200 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component.

Findings:	[ST] Section 6.7.2 includes table 21 which lists the TLS channels used and when the TOE is acting as the client or server. Section 6.7.2 also includes a list of claimed ciphersuites which match those claimed for the component. Additional, [ST] Section 6.7 describes the cryptographic functions being used in the Operational Environment. [ST] Section 2.5.3 lists the non-TOE components which compromise the operational environment. The [ST] only lists one platform.

5.3.2.2 Guidance Documentation

201 [Modified by TD0575] The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the product so that TLS conforms to the description in the TSS. If administrative steps need to be taken to disable a specific TLS application or so that the cipher suites negotiated by the implementation are limited to those in this requirement, then the appropriate instructions need to be contained in the guidance.

Findings:	The [AGD] specifies that the TOE will be configured with the support of the developer. This includes the configuration of the trusted channels and trusted paths. [AGD-Online] Appendix B Securing Communication provides guidance on the configuration of these services.

5.3.2.3 Tests

202 [Modified by TD0575 and TD0621] Test 1: The evaluator shall establish a TLS connection using each claimed cipher suite specified by the requirement. It is sufficient to observe the successful handshake following the negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to negotiate all specifically claimed ciphersuites.
Findings: PASS

203 Test 2: The evaluator shall perform the following modifications to the Client/Server Hellos:

204 Test 2a: [conditional on TOE implementing TLS client] The evaluator shall send a Server Hello containing only the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the TOE denies the connection.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server using TLS_NULL_WITH_NULL_NULL (cipher ID 0x0000).
Findings: PASS

205 Test 2b: [conditional on TOE implementing TLS Server] The evaluator shall send a Client Hello containing only the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the TOE denies the connection.

High-Level Test Description
Using a Lightship developed TLS client, force the TOE server to attempt a handshake with a test client using TLS_NULL_WITH_NULL_NULL (cipher ID 0x0000).
Findings: PASS

206 Test 3: The evaluator shall perform the following modifications to the traffic:

207 Test 3a: [conditional on TOE implementing TLS client]

208 Test 3a.1: Change the TLS version sent in the Server Hello to an undefined TLS version (for example 1.5 represented by the two bytes 03 06) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS server, connect to the TOE and attempt to negotiate an invalid TLS protocol version.
Findings: PASS

209 Test 3a.2: Change the TLS version sent in the Server Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS server, connect to the TOE and attempt to negotiate TLS 1.1 protocol and verify the TOE rejects the connection.
Findings: PASS

210 Test 3a.3: If DHE or ECDHE cipher suites are supported, modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the handshake is not completed and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a modified nonce value. Do this once for a DHE and ECDHE key exchange ciphersuite.
Findings: PASS

211 Test 3a.4: [conditional] If DHE or ECDHE cipher suites are supported, modify the signature block in the server's Key Exchange handshake message, and verify that the handshake does not complete and no application data flows. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled key exchange signature.
Findings: PASS

212 Test 3a.5:

213 Test 3a.5a: Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client does not complete the handshake and no application data flows.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a non-negotiated ciphersuite.
Findings: PASS

214 Test 3a.5b: Modify a byte in the Server Finished handshake message and verify the client does not complete the handshake and no application data flows.

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled finished message.
Findings: PASS

215 Test 3a.5c: Send a garbled message from the server after the server has issued the Change Cipher Spec message and verify that the client does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 …).

High-Level Test Description
Using a Lightship developed TLS server, force the TOE client to attempt a handshake with a test server sending a mangled message after the ChangeCipherSpec and verify no application data is sent.
Findings: PASS

216 **Test 3b**: [conditional on TOE implementing TLS server]

217 **Test 3b.1**: Change the TLS version sent in the Client Hello to the most recent unsupported TLS version (for example 1.1 represented by the two bytes 03 02) and verify that the TOE rejects the connection.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE and attempt to negotiate TLS 1.1 protocol and verify the TOE rejects the connection.
Findings: PASS

218 Test 3b.2:

219 **Test 3b.2a**: Modify a byte in the data of the client's Finished handshake message and verify the server rejects the connection and does not send any application data.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE and modify the first payload byte in the Client Finished message.
Findings: PASS

220 **Test 3b.2b**: Demonstrate that the TOE will not resume a session for which the client failed to complete the handshake (independent of TOE support for session resumption). Generate a Fatal Alert by sending a Finished message from the client before the client sends a ChangeCipherSpec message, and then send a ClientHello with the session identifier from the previous incomplete session and verify the server does not resume the session.

High-Level Test Description
Perform a successful handshake using one of the accepted ciphersuites and verify that the Server Finished message is encrypted.
Findings: PASS

221 **Test 3b.2c**: Send a garbled message from the client after the client has issued the Change Cipher Spec message and verify that the server does not complete the handshake and no application data flows. The garbled message must still have a valid 5-byte (1 byte record type, followed by 2 byte version, and 2 byte length) record layer header with matching version in order to ensure the message will be parsed appropriately. For example, for TLS v1.2 Change Cipher Spec (14 03 03 00 01 01) followed by a garbled message (16 03 03 00 40 14 00 00 …).

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE server and attempt a handshake with the test client sending a mangled message after the ChangeCipherSpec and verify no application data is sent.
Findings: PASS

6 Evaluation Activities for Security Assurance Requirements

6.1 Class ADV: Development

6.1.1 Basic Functional Specification (ADV_FSP.1)

222 There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

223 The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation.

Findings:	The evaluator reviewed the [ST], [AGD], and [AGD-Online] and found that they meet the assurance activities associated with the PP. They define the interfaces that the TOE uses, and invocation of those interfaces.

6.2 Class AGD: Guidance

6.2.1 Operational User Guidance (AGD_OPE.1)

224 Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.

225 The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

Findings:	The evaluator reviewed the [AGD-Online] and verified that the configuration of the cryptographic engine is specified. Appendix B.4 Enabling FIPS Mode on Oracle Access Management provides guidance on enabling FIPS mode on the TOE.

6.2.2 Preparative Procedures (AGD_PRE.1)

226 As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the

guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

Findings:	The [ST] specifies a single platform (Software and operating system combination). The guidance requirements for that platform have been assessed in this document.

6.3 Class ALC: Life Cycle Support

6.3.1 Labeling of the TOE (ALC_CMC.1)

227 The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Findings:	The evaluator reviewed the [ST] Section 1.1, the [AGD] Section 2 and [AGD-Online] Section “Get Started with Oracle Access Management”. The evaluator found that the TOE name and TOE version was specified, consistent, and sufficient to distinguish the product. The evaluator compared the TOE name and TOE version to the product and found it was consistent with the documentation.

6.3.2 TOE CM Coverage (ALC_CMS.1)

228 The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

Findings:	As noted in the assessment in Section 6.3.1 of this document the evaluator found the TOE name and TOE version to be consistent and sufficient to distinguish the TOE.

6.4 Class ATE: Tests

6.4.1 Independent Testing - Conformance (ATE_IND.1)

229 The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP’s Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators shall document in the test plan that each applicable testing requirement in the ST is covered.

230 The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between

the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

231 The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

232 The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.

Findings: The evaluator created a Test Plan which covers all of the testing actions contained in the body of this PP’s Assurance Activities. The Test Plan additionally provides the following information:

The platforms which are tested are specified in Section 2.1 Test Setup in the Test Plan.

The configuration of the platforms, a list of tested interfaces, and the tools used in the execution of the test plan are specified in the subsections of Section 2.1 Test Setup.

The high-level test objectives, test procedures, expected results, and actual results are included in the Test Plan.

The Test Plan has been created in a manner consistent with the PPs.

6.5 Class AVA: Vulnerability Assessment

6.5.1 Vulnerability Survey (AVA_VAN.1)

233 As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid

nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Findings: The evaluator conducted a public vulnerability survey searching for the TOE and TOE libraries. The evaluator documented the sources consulted and the potential vulnerabilities. The evaluator then reviewed the identified potential vulnerabilities for applicability to the TOE.

The evaluator found suitable vulnerabilities and performed tests in line with ATE_IND guidelines and provided justification for these vulnerabilities not existing or being mitigated.